

UNITED STATES DISTRICT COURT

for the
Western District of WashingtonIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)The person of Jeanne Rather, more fully described in
Attachment A

Case No. MJ21-041

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

The person of Jeanne Rather, more fully described in Attachments A, incorporated herein by reference.

located in the Western District of Washington, there is now concealed (identify the person or describe the property to be seized):

See Attachments B, incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:


Code Section	Offense Description
18 U.S.C. § 1028A	Aggravated Identity Theft
18 U.S.C. § 1344	Bank Fraud

The application is based on these facts:

- ☒ See Affidavit of Postal Inspector Anna Weller, continued on the attached sheet.

- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented: ☒ by reliable electronic means; or: ☐ telephonically recorded.



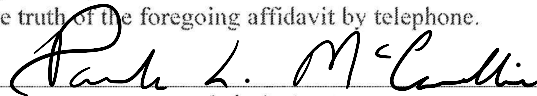
Applicant's signature

Anna Weller, Postal Inspector

Printed name and title

- ☐ The foregoing affidavit was sworn to before me and signed in my presence, or
☒ The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date: 01/25/2021



Judge's signature

City and state: Seattle, Washington

Paula L. McCandlis, United States Magistrate Judge

Printed name and title

3. My training includes, but is not limited to, the successful completion of the Basic Law Enforcement Academy through the Washington State Criminal Justice Training Commission and Basic Inspection Training through the Inspection Service Career Development Unit in Maryland. I have attended over 1000 hours of in-service training in the form of seminars, lectures, and classroom study to enhance my investigative knowledge and to stay current with any changes or advancements in law enforcement. I have also participated in and attended annual conferences held by the Northwest Fraud Investigators Association, the Financial Industry Mail Security Initiative, and the International Association of Financial Crimes Investigators. I have also completed Economic Crimes Training through the Department of Justice.

4. I make this affidavit from personal knowledge based on my participation in this investigation, including witness interviews by myself and/or other law enforcement agents, communications with others who have personal knowledge of the events and circumstances described herein, and information gained through my training and experience. The information outlined below is provided for the limited purpose of obtaining search warrants and does not contain all details or all facts of which I am aware relating to this investigation.

PURPOSE OF AFFIDAVIT

5. I make this affidavit in support of two applications for warrants authorizing the search of the following premises and person, which are further described below and in Attachments A to the respective applications (attached hereto and incorporated by reference as if fully set forth herein), for evidence, fruits and instrumentalities, as further described in Attachments B to the respective applications (attached hereto and incorporated by reference as if fully set forth herein), of the crimes of *Bank Fraud*, in violation of Title 18, United States Code, Section 1344, and *Aggravated Identity Theft*, in violation of Title 18, United States Code, Section 1028A, as described herein:

a. Fresenius Kidney Care, Skagit Valley, located at 208 Hospital Parkway Suite A, Mount Vernon, WA 98273 (hereinafter, the "SUBJECT

PREMISES”), described in more detail in Attachment A to that warrant, which is incorporated herein; and

b. The person of JEANNE RATHER (“RATHER”), described in more detail in Attachment A to that warrant, which is incorporated herein.

6. Since this Affidavit is intended to show only that there is a sufficient factual basis for a fair determination of probable cause to support the Applications, I have not included every fact known to me concerning this investigation. I have set forth only the facts that I believe are essential to establish the necessary foundation for search warrants for the SUBJECT PREMISES and RATHER.

STATEMENT OF PROBABLE CAUSE

7. The USPIS is currently conducting an investigation into JEANNE RATHER for violations of Title 18, United States Code, Section 1344 (bank fraud) and Title 18, United States Code, Section 1028A (aggravated identity theft), relating to credit cards issued by Capital One Bank (“Capital One”) in 2019. RATHER stole personally identifiable information (“PII”) from her victims, which she used to fraudulently obtain credit cards in the victims’ names from Capital One. RATHER then used these fraudulently obtained credit cards to make thousands of dollars in charges and defaulted on the payments, resulting in a total potential exposure of \$137,500 and total losses of \$106,089.57 to Capital One.

8. RATHER is the clinic coordinator at Fresenius Kidney Care, Skagit Valley (“Fresenius”), a dialysis clinic located at the SUBJECT PREMISES. A number of employees at Fresenius have learned that their PII, including their social security numbers and dates of birth, has been used to obtain credit cards from Capital One without their knowledge or authorization. According to one victim employee, RATHER’s position as Fresenius’s clinic coordinator would allow her to access employees’ personnel files, which would include the PII used to obtain credit cards in the victims’ names.

9. Records from Capital One relating to these credit card accounts and applications show that many of the unauthorized applications for credit cards in the

1 names of Fresenius employees are connected to RATHER and to other fraudulent
2 applications through overlapping mailing addresses, phone numbers, and/or IP addresses.
3 Moreover, transactions that have been completed using the credit cards demonstrate that
4 the charges to them were made by RATHER, including charges for airline tickets through
5 Alaska Air that were issued to RATHER and her family members.

6 **A. Identification of the Victims**

7 10. In July 2020, an investigator with Capital One contacted the USPIS
8 regarding an investigation into several fraudulent accounts that had been opened online.
9 The Capital One investigator had identified three credit cards that had been opened using
10 PII for three separate victims, each of which had been approved for a \$25,000 limit. The
11 Capital One investigator provided the USPIS with documentation showing that, after the
12 accounts had been opened in the victims' names, substantial charges had been made to
13 the cards, resulting in a total of \$67,041.01 in loss to Capital One.

14 11. Investigators with Capital One continued to investigate the fraudulent
15 accounts and later identified additional fraudulent accounts that had been opened using
16 other victims' PII, which are connected to RATHER or linked to known fraudulent
17 applications and accounts by overlapping mailing addresses, email accounts, and/or IP
18 addresses. In total, investigators with Capital One have identified seven fraudulent
19 accounts and five declined applications that investigators believe were submitted by
20 RATHER between September 5, 2019 and January 3, 2020. These fraudulent accounts
21 and applications were submitted using the PII of nine suspected victims, many of whom
22 are prior or current employees of Fresenius at the SUBJECT PREMISES.

23 12. All of the victims who had accounts opened in their names have filed fraud
24 reports with Capital One, notifying Capital One that they did not file the applications or
25 authorize anyone to do so on their behalf. I have interviewed two of these victims, who
26 both worked for Fresenius at the SUBJECT PREMISES and had Capital One accounts
27 opened in their names. Both of these victims confirmed that the accounts were
28 fraudulently opened, and that they had not authorized anyone to open the accounts on

1 their behalf. During the interview of one victim, K.E., she stated that RATHER was her
2 supervisor at Fresenius and thereby had access to her personal information. Moreover,
3 K.E. recognized the names of three other victims as her co-workers at Fresenius, where
4 she still works.

5 **B. Identification of RATHER**

6 13. Investigators with Capital One have provided the USPIS information
7 concerning the fraudulent applications for credit cards that are believed to be associated
8 with RATHER. These applications were submitted online, and Capital One collects and
9 has provided information regarding the date and time on which the application was
10 submitted, contact information provided at the time the application was submitted, and
11 the IP address from which the application was submitted. For applications that were
12 approved, Capital One has also provided USPIS with information regarding the
13 transactions conducted using the account, any payments made on the balance for the
14 account, and online activity for the account.

15 14. In reviewing information provided by Capital One, postal records, financial
16 records, databases, and publicly available information, I have found that the fraudulent
17 applications and accounts can be associated with RATHER through contact information
18 provided to Capital One at the time the application was submitted, IP addresses from
19 which the applications were submitted, and the transactions and payments made on the
20 accounts. The following examples are provided to illustrate the connections between
21 RATHER and the fraudulent applications, and they do not capture all of the evidence
22 showing that RATHER submitted the fraudulent applications that is known to me at this
23 time.

24 ***i. Mailing Addresses***

25 15. The information provided by Capital One shows that the mailing addresses
26 for almost all of the fraudulent applications can be associated with RATHER, either at
27 her known home address, two P.O. boxes that she has rented, or the SUBJECT
28 PREMISES (her place of work). For example, a total of six applications in victims'

1 names, including two that were approved, list P.O. Box 532 at the Marysville Post Office
2 as the mailing address.¹ Moreover, the mailing address for one account was changed to
3 P.O. Box 532 after the application was approved, and RATHER was added as an
4 authorized user of the account. According to post office records, RATHER is the user of
5 P.O. Box 532. She applied for the box on September 9, 2019, only one day before the
6 first fraudulent credit card application associated with this P.O. Box was submitted. The
7 application for the P.O. Box lists a home address that is associated with RATHER in
8 Snohomish County parcel records and a license plate number that is registered to her in
9 Department of Licensing records. P.O. Box 532 is also listed as the mailing address on a
10 Capital One account belonging to Stephen Rather, known to be RATHER's husband,
11 which is currently past due with a large balance. Finally, I have reviewed surveillance
12 footage from as recently as August 2020 and have seen a woman who appears to be
13 RATHER accessing P.O. Box 532.

14 16. In addition, two of the applications, including one that was approved, list
15 P.O. Box 578 at the Mount Vernon Post Office as the mailing address. According to post
16 office records, RATHER is the user of that P.O. Box. She applied for the box online,
17 listing Fresenius at the SUBJECT PREMISES as the business address. A printed version
18 of the application, likely used by an USPS employee to verify RATHER's identity when
19 she came to the post office to obtain the key to the P.O. Box, has RATHER's home
20 address in Marysville handwritten on it.

21 17. Finally, two other applications list the SUBJECT PREMISES, where many
22 of the victims have worked and where RATHER is the clinic coordinator, as a mailing
23 address.
24
25

26 ¹ Two of the applications list 1010 State Ave, Unit 532, Marysville, Washington, as the mailing
27 address. The Marysville Post Office is located at 1010 State Ave Marysville, WA and post
28 office boxes at the post office could be addressed directly to the PO Box or could list the actual
street address with the PO Box added as a unit number.

1 **ii. *Phone Numbers***

2 18. The information provided by Capital One further demonstrates that the
3 contact phone number for many of the fraudulent credit card applications can be
4 associated with RATHER. For example, K.E. provided contact phone numbers for
5 RATHER, listing her work cellular phone number as 360-403-6244, her personal cellular
6 phone number as 360-913-0002, and the clinic landline number as 360-336-2978. All of
7 these numbers are associated with at least one fraudulent credit card application. The
8 phone number 360-403-6244 is listed as the contact number for three applications,
9 including one that was approved. The phone number 360-913-0002 is listed as the home
10 number on three other fraudulent applications, including one that was approved. Finally,
11 the phone number 360-336-2978 is listed as the home number for one approved
12 application.

13 19. In addition to these phone numbers being associated with fraudulent
14 applications, they are also associated with activity for some of the fraudulent accounts.
15 The phone number 360-403-6244, RATHER's work cell number, accessed accounts
16 online and received SMS messages relating to two of the fraudulent accounts. The phone
17 number 360-913-0002, RATHER's personal cell number, received SMS messages
18 relating to one of the fraudulent accounts. Not surprisingly, the landline was not
19 associated with any online activity on any of the accounts, likely due to the fact that a
20 landline (versus a cellular phone) cannot be used to access websites or receive SMS
21 messages.

22 **iii. *Online Identifiers***

23 20. Capital One also provided investigators with information regarding online
24 activity for the fraudulent accounts and the IP addresses from which the fraudulent
25 applications were submitted, which connected several of the applications to each other
26 and provided further evidence that RATHER had submitted them. For example, in
27 September 2020, victim K.E. provided me with the IP address for the SUBJECT
28 PREMISES, 192.243.72.74. This IP address was used to submit four of the fraudulent

1 applications, two of which were approved, and was also used for several online logins to
2 three of the fraudulent accounts.

3 21. In addition to capturing the IP addresses of all online activity related to the
4 accounts and applications, Capital One also captures information relating to the date and
5 time of online activity, the device ID and name for the device used to access the accounts,
6 the action that was taken online, and the phone number associated with the online
7 activity. For three of the fraudulent accounts, Capital One's records show that they were
8 accessed online using the following devices: "iPhone (2)," "Jeanne's iPhone," and
9 "Jeanne's iPad." Both "iPhone (2)" and "Jeanne's iPhone" are associated with phone
10 numbers believed to be used by RATHER in Capital One's records.

11 ***iv. Fraudulent Transactions***

12 22. A review of the transactions on the fraudulent accounts show that a
13 majority of them were made in the Marysville area, where RATHER lives. Moreover,
14 over \$50,000 in charges were made to Pixie Fashion Outlet, an on-line clothing retail
15 store owned by RATHER. It appears that the domain name has expired, but as of July
16 23, 2020, I was able to access and view the business's website at
17 <https://pixiefashionoutlet.com>. The terms of service for the website listed RATHER's
18 home address in Marysville, Washington. Moreover, there is a Facebook profile with the
19 profile name "pixiefashionoutlet" that links to this website, and which is associated with
20 the phone number (360) 403-6244, believed to be RATHER's work cell phone number.
21 Based on my training and experience, I believe that RATHER made these fraudulent
22 charges to her own business in order to convert credit into a deposit into her bank
23 account, which would result in funds that she would more easily be able to use.

24 23. Transactions conducted on one of the fraudulent accounts show that the
25 user of the account purchased tickets for air travel from Alaska Air using the account.
26 An investigator for Capital One contacted Alaska Airlines, provided the airline with the
27 confirmation codes for the purchased tickets, and learned that the tickets were issued in
28 the names of RATHER, her husband, and her two children.

1 **C. The SUBJECT PREMISES**

2 24. Fresenius is part of the Fresenius Medical Care system and is located at the
3 SUBJECT PREMISES. The SUBJECT PREMISES is a kidney care clinic located in
4 Suite A of a one-story office building at Skagit Regional Health in the Hospital Parkway
5 Plaza. The office building is light grey in color with a covered walkway around the
6 southwest side, where the entrance and a parking lot are located. The building is affixed
7 with the numbers "208," and the words "Sonya Beard Hyperbaric Center," "Skagit
8 Wound Healing Center," and "Skagit Regional Clinics Nephrology" are stenciled on the
9 front window.

10 25. Inside the building is a small lobby, which is reached by going through the
11 entrance and passing through two sets of automatic sliding doors. On the eastern side of
12 this lobby is a set of glass double doors that open into the SUBJECT PREMISES,
13 labelled as "Fresenius Kidney Care" and with "Suite A" written above the doorway. I
14 have been inside of the building and am familiar with the entrance to the SUBJECT
15 PREMISES. Once inside the lobby area outside of the glass double doors, I was able to
16 see the door of RATHER's office, which is located in the reception area of the SUBJECT
17 PREMISES and is marked by a nametag next to the doorway identifying RATHER as the
18 Clinic Manager. At the time I visited the SUBJECT PREMISES, the door to RATHER's
19 office was open, and I was able to see what appeared to be the back of a computer
20 monitor through the doorway. I did not go any further into the SUBJECT PREMISES
21 but, based on my interview with K.E., I believe that RATHER has a work laptop that she
22 uses in her office, and which she may occasionally take home. K.E. also informed me
23 that the reception area has additional offices located off of it, used primarily by dietitians
24 and other medical personnel, and a coded door to the treatment floor where dialysis can
25 be administered to clinic clients.

26 26. Based on my interview of K.E., I have contact information for RATHER's
27 supervisor at Fresenius, who does not work at the SUBJECT PREMISES. I do not have
28 any information regarding this supervisor's knowledge of RATHER's fraud, or the

1 supervisor's relationship to RATHER, and have therefore not contacted this supervisor
2 regarding the investigation.

3 **D. Probable Cause**

4 27. There is probable cause to believe that evidence of RATHER's fraud will
5 be found at the SUBJECT PREMISES. Not only does it appear that RATHER has been
6 accessing and stealing her employees' PII at and from the SUBJECT PREMISES, but
7 Capital One's records show that Fresenius' IP address and phone number, and
8 RATHER's work phone, were used to apply for and access some of the fraudulent
9 accounts. Thereby, there is probable cause to believe that RATHER fraudulently applied
10 for credit card accounts through Capital One, sometimes while at the SUBJECT
11 PREMISES, and then later accessed those accounts while she was at the SUBJECT
12 PREMISES. This all could have been conducted on her work cellular phone, personal
13 cellular phone, work computer, a tablet, or another unknown device.

14 28. Moreover, there is probable cause to believe that RATHER utilized her
15 work computer to access the personal information of her employees with the intent of
16 committing identity theft. Based on my training and experience, most businesses keep
17 employee personal information in secure locations, either in paper format or on a secure
18 electronic device or network. Based on the investigation to date, there is probable cause
19 to believe that RATHER accessed her employees' personal information from such
20 locations, and that evidence of that fact will be found at the SUBJECT PREMISES.

21 29. Finally, there is probable cause to believe that evidence of RATHER's
22 fraud will be found on her personal cellular phone and/or work cellular phone. Records
23 from Capital One show that RATHER's personal cellular number and work number both
24 accessed fraudulent accounts online. Based on my training and experience, I know that
25 individuals often keep their cellular phones on their person or within reach. There is
26 therefore probable cause to believe that RATHER's cellular phones will be located on her
27 person.
28

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

29. As described above and in Attachments B, this application seeks permission to search for evidence, fruits and/or instrumentalities that might be found at the SUBJECT PREMISES, in whatever form they are found. One form in which the evidence, fruits, and/or instrumentalities might be found is data stored on digital devices² such as computer hard drives or other electronic storage media.³ Thus, the warrant applied for would authorize the seizure of digital devices or other electronic storage media or, potentially, the copying of electronically stored information from digital devices or other electronic storage media, all under Rule 41(e)(2)(B).

30. *Probable cause.* Based upon my review of the evidence gathered in this investigation, my review of data and records, information received from other agents and computer forensics examiners, and my training and experience, I submit that if a digital device or other electronic storage media is found at the SUBJECT PREMISES, there is probable cause to believe that evidence or fruits of the crimes of *Bank Fraud*, in violation of Title 18, United States Code, Section 1344, and *Aggravated Identity Theft*, in violation of Title 18, United States Code, Section 1028A, will be stored on those digital devices or other electronic storage media. Information uncovered in this investigation demonstrates that digital devices or other electronic storage media are being used by RATHER to access and store the victims' personal information, obtain fraudulent credit card

² "Digital device" includes any device capable of processing and/or storing data in electronic form, including, but not limited to: central processing units, laptop, desktop, notebook or tablet computers, computer servers, peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media, related communications devices such as modems, routers and switches, and electronic/digital security devices, wireless communication devices such as mobile or cellular telephones and telephone paging devices, personal data assistants ("PDAs"), iPods/iPads, Blackberries, digital cameras, digital gaming devices, global positioning satellite devices (GPS), or portable media players.

³ Electronic Storage media is any physical object upon which electronically stored information can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

1 applications in victims' names, use those credit cards to make purchases, and access the
2 credit card accounts. Information relating to the credit card applications and the
3 associated accounts further demonstrate that RATHER has used digital devices and
4 electronic storage media at the SUBJECT PREMISES to commit the crimes outlined
5 above. There is, therefore, probable cause to believe that evidence or fruits of the crimes
6 of *Bank Fraud*, in violation of Title 18, United States Code, Section 1344, and
7 *Aggravated Identity Theft*, in violation of Title 18, United States Code, Section 1028A,
8 exists and will be found on digital device or other electronic storage media at the
9 SUBJECT PREMISES, for at least the following reasons:

- 10 a. Based on my knowledge, training, and experience, I know that computer
11 files or remnants of such files can be preserved (and consequently also then
12 recovered) for months or even years after they have been downloaded onto
13 a storage medium, deleted, or accessed or viewed via the Internet.
14 Electronic files downloaded to a digital device or other electronic storage
15 medium can be stored for years at little or no cost. Even when files have
16 been deleted, they can be recovered months or years later using forensic
17 tools. This is so because when a person "deletes" a file on a digital device
18 or other electronic storage media, the data contained in the file does not
19 actually disappear; rather, that data remains on the storage medium until it
20 is overwritten by new data.
- 21 b. Therefore, deleted files, or remnants of deleted files, may reside in free
22 space or slack space—that is, in space on the digital device or other
23 electronic storage medium that is not currently being used by an active
24 file—for long periods of time before they are overwritten. In addition, a
25 computer's operating system may also keep a record of deleted data in a
26 "swap" or "recovery" file.
- 27 c. Wholly apart from user-generated files, computer storage media—in
28 particular, computers' internal hard drives—contain electronic evidence of
how a computer has been used, what it has been used for, and who has used
it. To give a few examples, this forensic evidence can take the form of
operating system configurations, artifacts from operating system or
application operation; file system data structures, and virtual memory
"swap" or paging files. Computer users typically do not erase or delete this
evidence, because special software is typically required for that task.
However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

31. *Forensic evidence.* As further described in Attachments B to the respective applications, these applications seek permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how digital devices or other electronic storage media were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any digital devices or other electronic storage media located at the SUBJECT PREMISES because:

a. Stored data can provide evidence of a file that was once on the digital device or other electronic storage media but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the digital device or other electronic storage media that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the history of connections to other computers, the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the digital device or other electronic storage media was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner and/or others

1 with direct physical access to the computer. Further, computer and storage
2 media activity can indicate how and when the computer or storage media was
3 accessed or used. For example, as described herein, computers typically
4 contain information that log: computer user account session times and
5 durations, computer activity associated with user accounts, electronic storage
6 media that connected with the computer, and the IP addresses through which
7 the computer accessed networks and the internet. Such information allows
8 investigators to understand the chronological context of computer or electronic
9 storage media access, use, and events relating to the crime under investigation.
10 Additionally, some information stored within a computer or electronic storage
11 media may provide crucial evidence relating to the physical location of other
12 evidence and the suspect. For example, images stored on a computer may both
13 show a particular location and have geolocation information incorporated into
14 its file data. Such file data typically also contains information indicating when
15 the file or image was created. The existence of such image files, along with
16 external device connection logs, may also indicate the presence of additional
17 electronic storage media (e.g., a digital camera or cellular phone with an
18 incorporated camera). The geographic and timeline information described
19 herein may either inculcate or exculpate the computer user. Last, information
20 stored within a computer may provide relevant insight into the computer user's
21 state of mind as it relates to the offense under investigation. For example,
22 information within the computer may indicate the owner's motive and intent to
23 commit a crime (e.g., internet searches indicating criminal planning), or
24 consciousness of guilt (e.g., running a "wiping" program to destroy evidence
25 on the computer or password protecting/encrypting such evidence in an effort
26 to conceal it from law enforcement).

19 c. A person with appropriate familiarity with how a digital device or other
20 electronic storage media works can, after examining this forensic evidence in
21 its proper context, draw conclusions about how the digital device or other
22 electronic storage media were used, the purpose of their use, who used them,
23 and when.

23 d. The process of identifying the exact files, blocks, registry entries, logs, or
24 other forms of forensic evidence on a digital device or other electronic storage
25 media that are necessary to draw an accurate conclusion is a dynamic process.
26 While it is possible to specify in advance the records to be sought, digital
27 evidence is not always data that can be merely reviewed by a review team and
28 passed along to investigators. Whether data stored on a computer is evidence
may depend on other information stored on the computer and the application of
knowledge about how a computer behaves. Therefore, contextual information

necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a digital device or other electronic storage media was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

32. Based on inspection of the spreadsheets provided by Capital One, I am aware that digital devices and other electronic storage media were used to generate, store, and/or print documents used in the fraud scheme, and to submit fraudulent applications for credit cards and to access accounts remotely. Moreover, based on victim interviews and physical surveillance of the SUBJECT PREMISES, there is reason to believe that there is a computer system currently located at the SUBJECT PREMISES.

PAST EFFORTS TO OBTAIN ELECTRONICALLY STORED INFORMATION

33. Because of the nature of the evidence that I am attempting to obtain and the covert nature of the investigation, including the fact that there does not appear to be an on-site supervisor at the clinic other than RATHER, I have not made any prior efforts to obtain the evidence based on the consent of any party who may have authority to consent. I believe, based upon the nature of the investigation and the information I have received, that if RATHER becomes aware of the investigation in advance of the execution of a search warrant, she may attempt to destroy any potential evidence, whether digital or non-digital, thereby hindering law enforcement agents from the furtherance of the criminal investigation.

REQUEST FOR AUTHORITY TO CONDUCT OFF-SITE SEARCH OF TARGET COMPUTERS

34. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of premises for information that might be stored on digital devices or other electronic storage media often requires the seizure of the physical items and later off-site review consistent with the warrant. In lieu of removing all of these

1 items from the premises, it is sometimes possible to make an image copy of the data on
 2 the digital devices or other electronic storage media, onsite. Generally speaking, imaging
 3 is the taking of a complete electronic picture of the device's data, including all hidden
 4 sectors and deleted files. Either seizure or imaging is often necessary to ensure the
 5 accuracy and completeness of data recorded on the item, and to prevent the loss of the
 6 data either from accidental or intentional destruction. This is true because of the
 7 following:

8 a. *The time required for an examination.* As noted above, not all evidence
 9 takes the form of documents and files that can be easily viewed on site.
 10 Analyzing evidence of how a computer has been used, what it has been used
 11 for, and who has used it requires considerable time, and taking that much time
 12 on premises could be unreasonable. As explained above, because the warrant
 13 calls for forensic electronic evidence, it is exceedingly likely that it will be
 14 necessary to thoroughly examine the respective digital device and/or electronic
 15 storage media to obtain evidence. Computer hard drives, digital devices and
 16 electronic storage media can store a large volume of information. Reviewing
 17 that information for things described in the warrant can take weeks or months,
 18 depending on the volume of data stored, and would be impractical and invasive
 19 to attempt on-site.

20 b. *Technical requirements.* Digital devices or other electronic storage media
 21 can be configured in several different ways, featuring a variety of different
 22 operating systems, application software, and configurations. Therefore,
 23 searching them sometimes requires tools or knowledge that might not be
 24 present on the search site. The vast array of computer hardware and software
 25 available makes it difficult to know before a search what tools or knowledge
 26 will be required to analyze the system and its data on the premises. However,
 27 taking the items off-site and reviewing them in a controlled environment will
 28 allow examination with the proper tools and knowledge.

29 c. *Variety of forms of electronic media.* Records sought under this warrant
 30 could be stored in a variety of electronic storage media formats and on a
 31 variety of digital devices that may require off-site reviewing with specialized
 32 forensic tools.

SEARCH TECHNIQUES

33 35. Based on the foregoing, and consistent with Rule 41(e)(2)(B) of the Federal
 34 Rules of Criminal Procedure, the warrants I am applying for will permit seizing, imaging,

1 or otherwise copying digital devices or other electronic storage media that reasonably
 2 appear capable of containing some or all of the data or items that fall within the scope of
 3 Attachments B to the respective warrants, and will specifically authorize a later review of
 4 the media or information consistent with the warrants.

5 36. Fresenius (“the Company”) is a functioning company that conducts
 6 legitimate business. The seizure of the Company’s computers may limit the Company’s
 7 ability to conduct its legitimate business. As with any search warrant, I expect that this
 8 warrant will be executed reasonably. Reasonable execution will likely involve
 9 conducting an investigation on the scene of what computers, or storage media, must be
 10 seized or copied, and what computers or storage media need not be seized or copied.
 11 Where appropriate, officers will copy data, rather than physically seize computers, to
 12 reduce the extent of disruption. If employees of the Company so request, the agents will,
 13 to the extent practicable, attempt to provide the employees with copies of data that may
 14 be necessary or important to the continuing function of the Company’s legitimate
 15 business. If, after inspecting the computers, it is determined that some or all of this
 16 equipment is no longer necessary to retrieve and preserve the evidence, the government
 17 will return it.

18 37. Consistent with the above, I hereby request the Court’s permission to seize
 19 and/or obtain a forensic image of digital devices or other electronic storage media that
 20 reasonably appear capable of containing data or items that fall within the scope of
 21 Attachments B to the respective applications and to conduct off-site searches of the
 22 digital devices or other electronic storage media and/or forensic images, using the
 23 following procedures:

24 **A. Processing the Search Sites and Securing the Data.**

25 a. Upon securing the physical search site, the search team will conduct an
 26 initial review of any digital devices or other electronic storage media located at
 27 the SUBJECT PREMISES described in Attachments A that are capable of
 28 containing data or items that fall within the scope of Attachments B to the
 respective warrants, to determine if it is possible to secure the data contained

1 on these devices onsite in a reasonable amount of time and without
2 jeopardizing the ability to accurately preserve the data.

3 b. In order to examine the electronically stored information (“ESI”) in a
4 forensically sound manner, law enforcement personnel with appropriate
5 expertise will attempt to produce a complete forensic image, if possible and
6 appropriate, of any digital device or other electronic storage media that is
7 capable of containing data or items that fall within the scope of Attachments B
8 to the respective warrants.⁴

9 c. A forensic image may be created of either a physical drive or a logical
10 drive. A physical drive is the actual physical hard drive that may be found in a
11 typical computer. When law enforcement creates a forensic image of a
12 physical drive, the image will contain every bit and byte on the physical drive.
13 A logical drive, also known as a partition, is a dedicated area on a physical
14 drive that may have a drive letter assigned (for example the c: and d: drives on
15 a computer that actually contains only one physical hard drive). Therefore,
16 creating an image of a logical drive does not include every bit and byte on the
17 physical drive. Law enforcement will only create an image of physical or
18 logical drives physically present on or within the subject device. Creating an
19 image of the devices located at the search locations described in Attachments
20 A will not result in access to any data physically located elsewhere. However,
21 digital devices or other electronic storage media at the search locations
22 described in Attachments A that have previously connected to devices at other
23 locations may contain data from those other locations.

24 d. If based on their training and experience, and the resources available to
25 them at the search site, the search team determines it is not practical to make an
26 on-site image within a reasonable amount of time and without jeopardizing the
27 ability to accurately preserve the data, then the digital devices or other
28

23 ⁴ The purpose of using specially trained computer forensic examiners to conduct the imaging of
24 digital devices or other electronic storage media is to ensure the integrity of the evidence and to
25 follow proper, forensically sound, scientific procedures. When the investigative agent is a
26 trained computer forensic examiner, it is not always necessary to separate these duties.
27 Computer forensic examiners often work closely with investigative personnel to assist
28 investigators in their search for digital evidence. Computer forensic examiners are needed
because they generally have technological expertise that investigative agents do not possess.
Computer forensic examiners, however, often lack the factual and investigative expertise that an
investigative agent may possess on any given case. Therefore, it is often important that
computer forensic examiners and investigative personnel work closely together.

1 electronic storage media will be seized and transported to an appropriate law
2 enforcement laboratory to be forensically imaged and reviewed.

3 **B. Searching the Forensic Images.**

4 a. Searching the forensic images for the items described in Attachments B
5 may require a range of data analysis techniques. In some cases, it is possible
6 for agents and analysts to conduct carefully targeted searches that can locate
7 evidence without requiring a time-consuming manual search through unrelated
8 materials that may be commingled with criminal evidence. In other cases,
9 however, such techniques may not yield the evidence described in the warrant,
10 and law enforcement may need to conduct more extensive searches to locate
11 evidence that falls within the scope of the warrant. The search techniques that
12 will be used will be only those methodologies, techniques and protocols as
13 may reasonably be expected to find, identify, segregate and/or duplicate the
14 items authorized to be seized pursuant to Attachments B to the respective
15 warrants. Those techniques, however, may necessarily expose many or all
16 parts of a hard drive to human inspection in order to determine whether it
17 contains evidence described by the warrant.

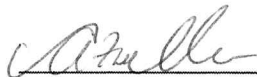
18 **REQUEST FOR SEALING**

19 30. It is respectfully requested that this Court issue an order sealing, until
20 further order of the Court, all papers submitted in support of these applications, including
21 the applications, this affidavit, and the search warrants. I believe that sealing this
22 document is necessary because the items and information to be seized are relevant to an
23 ongoing investigation and disclosure of the search warrants, this affidavit, and/or these
24 applications and the attachments thereto will jeopardize the progress of the investigation.
25 Disclosure of these materials would give the target of the investigation an opportunity to
26 destroy evidence, change patterns of behavior, notify confederates, or flee from
27 prosecution.

28 **CONCLUSION**

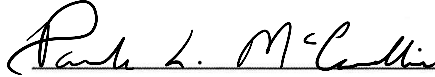
31. Based on the foregoing, I believe there is probable cause that evidence,
fruits, and instrumentalities of the crimes of *Bank Fraud*, in violation of Title 18, United
States Code, Section 1344, and *Aggravated Identity Theft*, in violation of Title 18, United
States Code, Section 1028A, are located at the SUBJECT PREMISES and on the person

1 of JEANNE RATHER, as more fully described in Attachments A to their respective
2 warrants. I therefore request that the court issue warrants authorizing the search of the
3 SUBJECT PREMISES and the person of JEANNE RATHER for the items more fully
4 described in Attachments B to their respective warrants, incorporated herein by reference,
5 and the seizure of any such items found therein.

6
7
8 

ANNA WELLER, Affiant
Postal Inspector, USPIS

10
11
12 The above-named agent provided a sworn statement attesting to the truth of the
13 foregoing affidavit by telephone on this 25th day of January, 2021.

14
15
16 

PAULA L. MCCANDLIS
United States Magistrate Judge